Available online at www.sciencedirect.com

ScienceDirect

Journal of Complexity 23 (2007) 581–593

Journal of COMPLEXITY

www.elsevier.com/locate/jco

# On the existence of higher order polynomial lattices based on a generalized figure of merit

Josef Dick[a], Peter Kritzer[b], Friedrich Pillichshammer[c], Wolfgang Ch. Schmid[b,*]

[a] *University of New South Wales Asia, 1 Kay Siang Road, Singapore 248922, Singapore*
[b] *Fachbereich Mathematik, Universität Salzburg, Hellbrunnerstraße 34, A-5020 Salzburg, Austria*
[c] *Institut für Finanzmathematik, Universität Linz, Altenbergerstraße 69, A-4040 Linz, Austria*

Received 9 October 2006; accepted 29 December 2006
Available online 30 January 2007

Dedicated to Henryk Woźniakowski on the occasion of his 60th birthday

**Abstract**

Dick and Pillichshammer recently introduced generalized rank-1 polynomial lattices which can be viewed as digital $(t, \alpha, \beta, n \times m, s)$-nets as introduced by the first author. In this work we generalize the figure of merit of rank-1 polynomial lattices such that the new figure of merit $\varrho_\alpha$ is related to the $t$-value, when one views the rank-1 polynomial lattice as a digital $(t, \alpha, \beta, n \times m, s)$-net. Then we show the existence of rank-1 polynomial lattices for which the generalized figure of merit $\varrho_\alpha$ satisfies a certain condition. We present some numerical results comparing the corresponding $t$-value to known explicit constructions.


*MSC:* 65D32; 65D30; 11K36

*Keywords:* Digital net; Polynomial lattice; Figure of merit

## 1. Introduction

Digital $(t, m, s)$-nets in base $b$ (see [8–11]) are useful for the numerical integration of functions with bounded variation over the high-dimensional unit cube. Recently, generalized digital nets (so-called digital $(t, \alpha, \beta, n \times m, s)$-nets in base $b$) were introduced in [2,3] which are also useful

* Corresponding author.
*E-mail addresses:* j.dick@unswasia.edu.sg (J. Dick), peter.kritzer@sbg.ac.at (P. Kritzer), friedrich.pillichshammer@jku.at (F. Pillichshammer), wolfgang.schmid@sbg.ac.at (W.Ch. Schmid).

0885-064X/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2006.12.003

for the numerical integration of smooth functions. First constructions of such generalized digital nets were also introduced in [2,3].

There is a subclass of "classical" digital nets called polynomial lattices [9,10], which was generalized in [4] to fit the new framework of $(t, \alpha, \beta, n \times m, s)$-nets introduced by the first author. Note that in this paper we only consider rank-1 polynomial lattices, but for short we refer to them as polynomial lattices. Various results on the existence of such polynomial lattices are known for the classical case [5,12] and in this paper we show results on the existence of polynomial lattices within the new framework depending on their digital $(t, \alpha, \beta, n \times m, s)$-net properties (the precise definition of such digital nets will be given below). In particular, a result which relates the $t$-value of a classical polynomial lattice to its figure of merit $\rho$ [10], is generalized here to a relation between the type of digital nets considered in [2,3] and the polynomial lattices introduced in [4]. More precisely, we generalize the figure of merit $\rho$ to higher orders $\alpha > 1$ and relate it to the $t$-value when one considers those polynomial lattices as digital $(t, \alpha, \beta, n \times m, s)$-nets.

The relevance of such constructions for numerical integration will be explained in the following.

Consider the Sobolev space $\mathcal{H}_{\mathrm{sob},s,\delta}$ of functions $f : [0, 1]^s \to \mathbb{R}$ whose partial mixed derivatives up to order $\delta$ in each variable are square integrable. Here $s \geqslant 1$ and $\delta > 1$ (for $\delta = 1$ we obtain the classical case which has been considered in many papers, see for example [10,14] and the references therein). For the one-dimensional case the inner product is given by

$$\langle f, g\rangle_{\mathcal{H}_{\mathrm{sob},1,\delta}} = \sum_{\tau=0}^{\delta-1} \int_0^1 f^{(\tau)}(x)\,\mathrm{d}x \int_0^1 g^{(\tau)}(x)\,\mathrm{d}x + \int_0^1 f^{(\delta)}(x) g^{(\delta)}(x)\,\mathrm{d}x,$$

where $f^{(\tau)}$ denotes the $\tau$th derivative of $f$ and where $f^{(0)} = f$. The reproducing kernel (see [1] for more information about reproducing kernels) for this space is given by

$$\mathcal{K}_{\mathrm{sob},1,\delta}(x, y) = \sum_{\tau=0}^{\delta} \frac{B_\tau(x) B_\tau(y)}{(\tau!)^2} + \frac{B_{2\delta}(|x - y|)}{(2\delta)!},$$

where $B_\tau$ denotes the Bernoulli polynomial of degree $\tau$, e.g., we have $B_0(x) = 1$, $B_1(x) = x - 1/2$, $B_2(x) = x^2 - x + 1/6$ and so on. For dimension $s > 1$, $\mathcal{H}_{\mathrm{sob},s,\delta}$ refers to the tensor product of $s$ such one-dimensional spaces.

In [14] the authors introduced the notion of weighted function spaces. To this end they introduced a sequence $\boldsymbol{\gamma} = \{\gamma_u : u \subseteq \{1, \ldots, s\}\}$ of positive weights to model the importance of different coordinate directions of the integrand. For an exact definition of the weighted version $\mathcal{H}_{\mathrm{sob},s,\delta,\boldsymbol{\gamma}}$ of the function space $\mathcal{H}_{\mathrm{sob},s,\delta}$ and for more information on those or related spaces in our context we refer to [3] (see also [2] for a version for periodic functions).

Consider now numerical integration of functions from the weighted Sobolev space $\mathcal{H}_{\mathrm{sob},s,\delta,\boldsymbol{\gamma}}$ by a quasi-Monte Carlo rule $Q_{b^m,s}$ based on digital nets, i.e., an equal weight quadrature rule with the quadrature points taken from a digital net consisting of $b^m$ points. We measure the quality of the quadrature points using the worst-case error $e(Q_{b^m,s}, \mathcal{H}_{\mathrm{sob},s,\delta,\boldsymbol{\gamma}})$, which is the worst performance of our quasi-Monte Carlo rule $Q_{b^m,s}$ over all functions in the unit ball in the Sobolev space $\mathcal{H}_{\mathrm{sob},s,\delta,\boldsymbol{\gamma}}$. Using these notations, the following theorem was shown in [3].

**Theorem 1.** *Let $\delta > 1$ be an integer and $b \geqslant 2$ be a prime number. The worst-case error for multivariate integration in the Sobolev space $\mathcal{H}_{\mathrm{sob},s,\delta,\boldsymbol{\gamma}}$, using a digital $(t, \delta, \beta, n \times m, s)$-net*

*over* $\mathbb{F}_b$ *(with* $0 < \beta \leqslant 1$*) as quadrature points, is bounded by*

$$e(Q_{b^m,s}, \mathcal{H}_{\mathrm{sob},s,\delta,\gamma}) \leqslant b^{-(\beta n - t)} \left( \sum_{\emptyset \neq u \subseteq \{1,\ldots,s\}} \gamma_u (C''_{|u|,b,\delta})^2 (\beta n - t + \delta)^{2|u|\delta} \right)^{1/2},$$

*where*

$$C''_{|u|,b,\delta} = C_{b,\delta}^{|u|/2} b^{|u|\delta} \left( b^{-1} + \left(1 - b^{1/\delta - 1}\right)^{-|u|\delta} \right)$$

*and* $C_{b,\delta} > 0$ *is a constant depending only on b and* $\delta$*.*

Among other things, in [3] it was shown that for each $\alpha$, $m$ and $s$ there is a digital $(t, \alpha, 1, \alpha m \times m, s)$-net (i.e., $\beta = 1$ and $n = \alpha m$) and that one can explicitly construct such digital nets with the $t$-value being independent of $m$. By using such a digital $(t, \alpha, 1, \alpha m \times m, s)$-net with $\alpha \geqslant \delta$ one can obtain a convergence rate of order $N^{-\delta}(\log N)^{s\delta}$ (where $N = b^m$ denotes the number of points), see [3] (and also [2] for similar results). Note that the $t$-value is a quality parameter of such digital nets (see below for the precise definitions). Smaller values of $t$ imply better bounds on the worst-case error (compare with Theorem 1).

The aim of this paper is to show that computer search methods for finding good digital $(t, \alpha, \beta, n \times m, s)$-nets (via generalized polynomial lattices) can be useful. More precisely, we show here that for certain values of $\alpha, n, m, s, b$ we can find digital $(t, \alpha, \beta, n \times m, s)$-nets using computer search based on generalized rank-1 polynomial lattices with a lower $t$-value than the known constructions from [2,3]. As for classical $(t, m, s)$-nets in base $b$ there are purely theoretical constructions, but for some parameters $m, s, b$ computer search methods provide nets with smaller $t$-value, i.e., higher quality (see the web-based database system MINT available at the address `http://mint.sbg.ac.at/`). As will be shown in this paper, the same happens for the generalized digital nets introduced in [2,3]. Unfortunately, our results here are not explicit as opposed to the constructions in [2,3]. On the other hand our results here show that there is still room for improvement upon the constructions for digital nets proposed in [2,3] (though the same cannot be inferred from our paper for digital sequences). Just as for classical polynomial lattices, the asymptotic results on the $t$-value are not as good as the ones from theoretical constructions, see [5] for the classical case, which also appears in our case here. Hence the improvement upon the theoretical constructions is not in general terms (i.e., asymptotically) but rather for specific instances of $\alpha, n, m, s$ and $b$.

At the end of the paper we give numerical results comparing the $t$-values obtained in this paper with the ones obtained using the construction in [2,3] based on known explicit constructions. From there one can see that in some cases computer search methods can produce digital nets of higher quality than one can obtain from the explicit constructions proposed in [2,3].

## 2. Digital nets and polynomial lattices

In this section we introduce digital nets and polynomial lattices which can achieve arbitrary high convergence rates of the integration error for suitably smooth functions (see [2,3]). This is achieved by a slight generalization of the classical definition of digital nets (i.e., we consider generating matrices of size $n \times m$ instead of $m \times m$), see [8–10], and [11] for a recent survey article on digital nets.

In the following let $b$ be a prime and let $\mathbb{F}_b$ denote the finite field of order $b$.

**Definition 1** (*Digital net*). Let $b$ be a prime and let $s, m, n \geqslant 1$ be integers. Let $C_1, \ldots, C_s$ be $n \times m$ matrices over the finite field $\mathbb{F}_b$. We construct $b^m$ points in $[0, 1)^s$ in the following way: for $0 \leqslant h < b^m$ let $h = h_0 + h_1 b + \cdots + h_{m-1} b^{m-1}$ be the $b$-adic expansion of $h$. Identify $h$ with the vector $\vec{h} = (h_0, \ldots, h_{m-1})^\top \in \mathbb{F}_b^m$, where $\top$ means the transpose of the vector. For $1 \leqslant j \leqslant s$ multiply the matrix $C_j$ by $\vec{h}$, i.e.,

$$C_j \vec{h} =: (y_{j,1}(h), \ldots, y_{j,n}(h))^\top \in \mathbb{F}_b^n,$$

and set

$$x_{h,j} := \frac{y_{j,1}(h)}{b} + \cdots + \frac{y_{j,n}(h)}{b^n}.$$

The point set $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{b^m-1}\}$ with $\boldsymbol{x}_h = \left(x_{h,1}, \ldots, x_{h,s}\right)$ is called a digital net (over $\mathbb{F}_b$) (with generating matrices $C_1, \ldots, C_s$).

The following definition was first introduced in [3] (see also [2] for a similar definition). It is fitted to the behavior of the Walsh coefficients of smooth functions via the dual net in order to obtain a fast convergence of the integration error for numerical integration using this type of digital net. For details see [2,3].

**Definition 2** (*Digital* $(t, \alpha, \beta, n \times m, s)$*-net*). Let $n, m, \alpha \geqslant 1$ be natural numbers, let $0 < \beta \leqslant \alpha m/n$ be a real number and let $0 \leqslant t \leqslant \beta n$ be a natural number. Let $C_1, \ldots, C_s \in \mathbb{F}_b^{n \times m}$ with $C_j = (c_{j,1}, \ldots, c_{j,n})^\top$ and $c_{j,i} \in \mathbb{F}_b^m$. If for all $1 \leqslant i_{j,v_j} < \cdots < i_{j,1} \leqslant n$, where $0 \leqslant v_j \leqslant n$ for all $j = 1, \ldots, s$, with

$$i_{1,1} + \cdots + i_{1,\min(v_1,\alpha)} + \cdots + i_{s,1} + \cdots + i_{s,\min(v_s,\alpha)} \leqslant \beta n - t$$

the vectors

$$c_{1,i_{1,v_1}}, \ldots, c_{1,i_{1,1}}, \ldots, c_{s,i_{s,v_s}}, \ldots, c_{s,i_{s,1}}$$

are linearly independent over $\mathbb{F}_b$ then the digital net with generating matrices $C_1, \ldots, C_s$ is called a digital $(t, \alpha, \beta, n \times m, s)$-net over $\mathbb{F}_b$. Further we call a digital $(t, \alpha, 1, \alpha m \times m, s)$-net over $\mathbb{F}_b$ a digital $(t, \alpha, \alpha m \times m, s)$-net over $\mathbb{F}_b$.

For $\alpha = \beta = 1$ and $n = m$ in the definition above we obtain the classical definition of digital $(t, m, s)$-nets over $\mathbb{F}_b$, see [10], i.e., a digital $(t, 1, 1, m \times m, s)$-net over $\mathbb{F}_b$ is a digital $(t, m, s)$-net over $\mathbb{F}_b$.

Note that for $(t, m, s)$-nets the value of $t$ gives information about the quality of the net, whereas $m$ refers to the number of points given by $b^m$ and $s$ to the dimension. For digital $(t, \alpha, \beta, n \times m, s)$-nets, $t$, $m$ and $s$ have the same meaning as for the classical case. Additionally, $\alpha$ refers to the order of the digital net, $n$ to the depth (i.e., maximum number of non-zero digits in the base $b$ representation a coordinate of a point can have) and $\beta$ relates to the convergence order such a point set can achieve when integrating a function of smoothness at least $\delta$ (i.e., for example, square integrable partial mixed derivatives of order $\delta$ in each variable).

In [9] (see also [10, Section 4.4]) Niederreiter introduced a special family of digital nets over $\mathbb{F}_b$. Those nets are obtained from rational functions over finite fields. For a prime $b$ let $\mathbb{F}_b((x^{-1}))$

be the field of formal Laurent series over $\mathbb{F}_b$. Elements of $\mathbb{F}_b((x^{-1}))$ are formal Laurent series,

$$L = \sum_{l=w}^{\infty} t_l x^{-l},$$

where $w$ is an arbitrary integer and all $t_l \in \mathbb{F}_b$. Note that $\mathbb{F}_b((x^{-1}))$ contains the field of rational functions over $\mathbb{F}_b$ as a subfield. Further, let $\mathbb{F}_b[x]$ be the set of all polynomials over $\mathbb{F}_b$.

The following definition is a slight generalization of the definition from [9], see also [10]. A special case of this definition was considered in [4].

**Definition 3** (*Rank-1 Polynomial lattice*). For a given dimension $s \geqslant 1$, choose $p \in \mathbb{F}_b[x]$ with $\deg(p) = n \geqslant 1$ and let $\boldsymbol{q} = (q_1, \ldots, q_s) \in \mathbb{F}_b^s[x]$. Define matrices $C_1, \ldots, C_s \in \mathbb{F}_b^{n\times m}$ in the following way: for $1 \leqslant j \leqslant s$, consider the expansions

$$\frac{q_j(x)}{p(x)} = \sum_{l=w_j}^{\infty} u_l^{(j)} x^{-l} \in \mathbb{F}_b((x^{-1})),$$

where $w_j \in \mathbb{Z}$. Then the elements $c_{i,r}^{(j)}$ of the $n \times m$ matrix $C_j$ over $\mathbb{F}_b$ are given by

$$c_{i,r}^{(j)} = u_{r+i}^{(j)} \in \mathbb{F}_b,$$

for $1 \leqslant j \leqslant s$, $1 \leqslant i \leqslant n$, $0 \leqslant r \leqslant m-1$. The digital net $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ over $\mathbb{F}_b$ with generating matrices $C_1, \ldots, C_s$ is called a rank-1 polynomial lattice.

In the following we will write polynomial lattice to abbreviate rank-1 polynomial lattice. (For higher rank polynomial lattices see [6,7].)

**Remark 1.** For the case considered above there is also an equivalent but simpler definition of a polynomial lattice. Let $\upsilon_n$ be the map from $\mathbb{F}_b((x^{-1}))$ to the interval $[0, 1)$ defined by

$$\upsilon_n\left(\sum_{l=w}^{\infty} t_l x^{-l}\right) = \sum_{l=\max(1,w)}^{n} t_l b^{-l}.$$

For a given dimension $s \geqslant 1$, choose $p \in \mathbb{F}_b[x]$ with $\deg(p) = n \geqslant 1$ and let $q_1, \ldots, q_s \in \mathbb{F}_b[x]$. For $0 \leqslant h < b^m$ let $h = h_0 + h_1 b + \cdots + h_{m-1} b^{m-1}$ be the $b$-adic expansion of $h$. With each such $h$ we associate the polynomial

$$h(x) = \sum_{r=0}^{m-1} h_r x^r \in \mathbb{F}_b[x].$$

Then the polynomial lattice $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ is the point set consisting of the $b^m$ points

$$\boldsymbol{x}_h = \left(\upsilon_n\left(\frac{h(x)q_1(x)}{p(x)}\right), \ldots, \upsilon_n\left(\frac{h(x)q_s(x)}{p(x)}\right)\right) \in [0, 1)^s,$$

for $0 \leqslant h < b^m$.

A quasi-Monte Carlo rule using the point set $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ is called a polynomial lattice rule.

**Remark 2.** The point set $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ consists of the first $b^m$ points of $\mathcal{S}_{p,n,n}(\boldsymbol{q})$, i.e., the first $b^m$ points of a classical polynomial lattice (i.e., as defined in [9]). Hence the definition of a polynomial lattice in [9] is covered by choosing $n = m$ in the definition above.

Finally we introduce some notation: for arbitrary $\boldsymbol{k}=(k_1, \ldots, k_s)\in\mathbb{F}_b^s[x]$ and $\boldsymbol{q}=(q_1, \ldots, q_s) \in \mathbb{F}_b^s[x]$, we define the 'inner product'

$$\boldsymbol{k} \cdot \boldsymbol{q} = \sum_{j=1}^{s} k_j q_j \in \mathbb{F}_b[x]$$

and we write $q \equiv 0 \pmod p$ if $p$ divides $q$ in $\mathbb{F}_b[x]$. Further, we associate a non-negative integer $k$ with base $b$ representation $k = \kappa_0 + \kappa_1 b + \cdots + \kappa_a b^a$ with the polynomial $k(x) = \kappa_0 + \kappa_1 x + \cdots + \kappa_a x^a \in \mathbb{F}_b[x]$ and vice versa.

For polynomial lattices with $n = m$ a connection between the figure of merit and the $t$-value, when one views $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ as a digital $(t, m, s)$-net over $\mathbb{F}_b$, was established, see [10]. In the following we generalize these results.

First let us generalize the figure of merit of a polynomial lattice. Let $k(x) = \kappa_0 + \kappa_1 x + \cdots + \kappa_a x^a \in \mathbb{F}_b[x]$ with $\kappa_a \neq 0$. Then the degree of the polynomial $k$ is defined by $\deg(k) = a$ and for $k = 0$ we set $\deg(k) = -1$. For our purposes we need to generalize this definition. Let $k(x) = \kappa_v x^{a_v-1} + \cdots + \kappa_1 x^{a_1-1}$ with $\kappa_1, \ldots, \kappa_v \in \mathbb{F}_b \setminus \{0\}$ and $0 < a_v < \cdots < a_1$. For $\alpha \geqslant 1$ we now set $\deg_\alpha(k) = \sum_{r=1}^{\min(v,\alpha)} a_r$ and for $k = 0$ we set $\deg_\alpha(k) = 0$. Thus we have, for example, $\deg_1(k) = \deg(k) + 1$. In what follows we will call $\deg_\alpha(k)$ the $\alpha$-degree of the polynomial $k$. Using this notation we can now generalize the classical definition of the figure of merit [10, Definition 4.39].

**Definition 4** (*Figure of merit*). Let $p \in \mathbb{F}_b[x]$ with $\deg(p) = n$ and let $\boldsymbol{q} \in \mathbb{F}_b^s[x]$ be the generating vector of a polynomial lattice $\mathcal{S}_{p,m,n}(\boldsymbol{q})$. For $\alpha \geqslant 1$ the figure of merit $\varrho_\alpha$ is given by

$$\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) = -1 + \min \sum_{j=1}^{s} \deg_\alpha(k_j),$$

where the minimum is extended over all non-zero $\boldsymbol{k} \in \mathbb{F}_b^s[x]$ with $\deg(k_j) < n$ for $1 \leqslant j \leqslant s$ and where there is a polynomial $a \in \mathbb{F}_b[x]$ with $a \equiv \boldsymbol{q} \cdot \boldsymbol{k} \pmod p$ and $\deg(a) < n - m$.

Note that for $n = m$ and $\alpha = 1$ we obtain the classical definition of the figure of merit, see [10, Definition 4.39]. (We remark that other generalizations of quality measures have been considered in [6,7], but they do not deal with higher order convergence for the numerical integration of smooth functions.)

Let $\boldsymbol{q} \in \mathbb{F}_b^s[x]$ be a generating vector for a polynomial lattice and let $p \in \mathbb{F}_b[x]$ with $\deg(p) = n$. Let $C_1, \ldots, C_s \in \mathbb{F}_b^{n\times m}$ denote the corresponding generating matrices. A slight generalization of [10, Lemma 4.40], see also [4], yields now that

$$C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s = \vec{0} \in \mathbb{F}_b^m,$$

if and only if there is a polynomial $a \in \mathbb{F}_b[x]$ with $a \equiv \boldsymbol{q} \cdot \boldsymbol{k} \pmod p$ and $\deg(a) < n - m$. Here $\vec{k}_j = (\kappa_{j,0}, \ldots, \kappa_{j,n-1})^\top \in \mathbb{F}_b^n$, $\bar{k}_j(x) = \kappa_{j,0} + \kappa_{j,1} x + \cdots + \kappa_{j,n-1} x^{n-1} \in \mathbb{F}_b[x]$ and $\boldsymbol{k} = (\bar{k}_1, \ldots, \bar{k}_s)$. Using this result, also [10, Corollary 4.41] and [10, Theorem 4.42] can be generalized to yield the following theorem.

**Theorem 2.** *Let $p \in \mathbb{F}_b[x]$ with $\deg(p) = n$ and let $\boldsymbol{q} \in \mathbb{F}_b^s[x]$ be the generating vector of a polynomial lattice $\mathcal{S}_{p,m,n}(\boldsymbol{q})$. Then $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ is a digital $(t, \alpha, \beta, n \times m, s)$-net over $\mathbb{F}_b$ for any $0 < \beta \leqslant \alpha m/n$ and $0 \leqslant t \leqslant \beta n$ which satisfy*

$$t = \lfloor \beta n \rfloor - \varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})).$$

We see that polynomial lattices of high quality have a large value of $\varrho_\alpha$. In the following section we show the existence of polynomial lattices for which $\varrho_\alpha$ satisfies a certain condition.

## 3. On the existence of polynomial lattices based on the figure of merit

In this section we use the approach of [5] to prove the existence of polynomial lattices for which the figure of merit satisfies a certain condition. First note that we can restrict $\boldsymbol{q} \in \mathbb{F}_b^s[x]$ to the set $R_n^s$ where $R_n$ denotes the set of all polynomials $q \in \mathbb{F}_b[x]$ with $\deg(q) < n$.

The following lemma gives an upper bound on the number of polynomials in $R_n$ with a given $\alpha$-degree. Note that we will use the convention $\binom{n}{k} = 0$ for negative integers $n$.

**Lemma 1.** *Let $l, \alpha, n \geqslant 1$ be natural numbers. Then the number of polynomials in $R_n$ with $\alpha$-degree $l$ is bounded by*

$$\#\{k \in R_n : \deg_\alpha(k) = l\} \leqslant C(\alpha, l),$$

*where*

$$C(\alpha, l) = \sum_{v=1}^{\alpha-1} (b-1)^v \binom{l - \frac{v(v-1)}{2} - 1}{v-1} + \sum_{i=1}^{\lfloor l/\alpha \rfloor} (b-1)^\alpha b^{i-1} \binom{l - \alpha \cdot i - \frac{\alpha(\alpha-3)}{2} - 2}{\alpha - 2}.$$

**Proof.** Let $k \in R_n$, $k = k_{a_v} x^{a_v - 1} + \cdots + k_{a_1} x^{a_1 - 1}$ with $0 < a_v < \cdots < a_1$ and $k_{a_r} \neq 0$ for $r \in \{1, \ldots, v\}$. The $\alpha$-degree of $k$ is then given by $\deg_\alpha(k) = \sum_{r=1}^{\min(v,\alpha)} a_r$.

We consider two cases:

(1) $\alpha \leqslant v$: Then we write

$$k = k_{a_1} x^{a_1 - 1} + \cdots + k_{a_\alpha} x^{a_\alpha - 1} + k_{a_\alpha - 1} x^{a_\alpha - 2} + \cdots + k_2 x + k_1.$$

As in this case only $a_1, \ldots, a_\alpha$ appear in the condition for the $\alpha$ degree of $k$, we can choose the part $k_{a_\alpha - 1} x^{a_\alpha - 2} + \cdots + k_2 x + k_1$ arbitrarily and hence we have at most $b^{a_\alpha - 1}$ possibilities for this part. Further the $k_{a_r}$ need to be non-zero such that we have at all $(b-1)^\alpha$ possible choices. Now we have to count the number of $a_1, \ldots, a_\alpha$ with $0 < a_\alpha < \cdots < a_1$ and $a_1 + \cdots + a_\alpha = l$ or equivalently $(a_1 - a_\alpha) + \cdots + (a_{\alpha-1} - a_\alpha) = l - \alpha a_\alpha$. (Note that $l - \alpha a_\alpha$ must be at least non-negative.) This is the same as the number of $0 \leqslant b_{\alpha-1} \leqslant \cdots \leqslant b_1$ with $b_1 + \cdots + b_{\alpha-1} = l - \alpha a_\alpha - \frac{\alpha(\alpha-1)}{2}$; write $b_i = a_i - a_\alpha - (\alpha - i)$ for $i = 1, \ldots, \alpha - 1$. However, this number is surely at most $\binom{l - \alpha a_\alpha - \frac{\alpha(\alpha-1)}{2} + \alpha - 2}{\alpha - 2}$.

Finally, $a_\alpha$ can run from 1 to at most $\lfloor l/\alpha \rfloor$ and hence altogether there are at most

$$\sum_{a_\alpha=1}^{\lfloor l/\alpha \rfloor} (b-1)^\alpha b^{a_\alpha - 1} \binom{l - \alpha a_\alpha - \frac{\alpha(\alpha-1)}{2} + \alpha - 2}{\alpha - 2}$$

polynomials $k = k_{a_v} x^{a_v - 1} + \cdots + k_{a_1} x^{a_1 - 1}$ with $0 < a_v < \cdots < a_1$ and $k_{a_r} \neq 0$ for $r \in \{1, \ldots, v\}$, $\alpha \leqslant v$ and $\deg_\alpha(k) = l$.

(2) $\alpha > v$: We count all $k = k_{a_v} x^{a_v - 1} + \cdots + k_{a_1} x^{a_1 - 1}$ with $0 < a_v < \cdots < a_1$, $k_{a_r} \neq 0$ for $r \in \{1, \ldots, v\}$ and $a_1 + \cdots + a_v = l$.
For $k_{a_r}$, $r \in \{1, \ldots, v\}$ we have exactly $(b-1)^v$ possible choices. The number of $0 < a_v < \cdots < a_1$ with $a_1 + \cdots + a_v = l$ is the same as the number of $0 \leqslant b_v \leqslant \cdots \leqslant b_1$ with $b_1 + \cdots + b_v = l - \frac{v(v+1)}{2}$; write $b_i = a_i - (v + 1 - i)$ for $i = 1, \ldots, v$. This number can be bounded from above by $\binom{l - \frac{v(v+1)}{2} + v - 1}{v-1}$. As $v$ may be chosen from $\{1, \ldots, \alpha - 1\}$ we have at most

$$\sum_{v=1}^{\alpha-1} (b-1)^v \binom{l - \frac{v(v+1)}{2} + v - 1}{v - 1}$$

polynomials $k = k_{a_v} x^{a_v - 1} + \cdots + k_{a_1} x^{a_1 - 1}$ with $0 < a_v < \cdots < a_1$ and $k_{a_r} \neq 0$ for $r \in \{1, \ldots, v\}$, $\alpha > v$ and $\deg_\alpha(k) = l$.

The result follows by adding the two sums from the above two cases. □

Now we can prove our main result which gives a condition for the existence of a polynomial lattice with a certain figure of merit.

**Theorem 3.** *Let $n, m, \alpha \geqslant 1$, $s \geqslant 2$ be natural numbers, $b$ a prime and $p \in \mathbb{F}_b[x]$ with $\deg(p) = n \geqslant m$ be irreducible. For $\varrho > 0$ define*

$$\Delta(s, \varrho, \alpha) = \sum_{l=0}^{\varrho} \sum_{i=1}^{s} \binom{s}{i} \sum_{\substack{l_1, \ldots, l_i \geqslant 1 \\ l_1 + \cdots + l_i = l}} \prod_{z=1}^{i} C(\alpha, l_z),$$

*where $C(\alpha, l)$ is defined in Lemma* 1.

(1) *If $\Delta(s, \varrho, \alpha) < b^m$, then there exists a $\boldsymbol{q} \in R_n^s$ with*

$$\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \varrho.$$

(2) *If $\Delta(s, \varrho, \alpha) < \frac{b^m}{s-1}$, then there exists a polynomial $q \in R_n$ such that $\boldsymbol{q} \equiv (1, q, q^2, \ldots, q^{s-1}) \pmod p$ satisfies*

$$\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \varrho.$$

**Proof.** (1) There are $|R_n^s| = |R_n|^s = b^{ns}$ vectors $\boldsymbol{q}$ to choose from. We will estimate the number of vectors $\boldsymbol{q}$ for which $\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) < \varrho$ for some chosen $\varrho \geqslant 0$. If this number is smaller than the total number of possible choices then it follows that there is at least one vector with $\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \varrho$.

For each non-zero vector $\boldsymbol{k} \in \mathbb{F}_b^s[x]$ there are $b^{ns-m}$ vectors $\boldsymbol{q} \in R_n^s$ such that $\boldsymbol{k} \cdot \boldsymbol{q} \equiv a \pmod p$ for some $a \in \mathbb{F}_b[x]$ with $\deg(a) < n - m$.

Let now $A(l, s, \alpha)$ denote the number of non-zero vectors $\boldsymbol{k} \in \mathbb{F}_b^s[x]$ with $\sum_{j=1}^s \deg_\alpha(k_j) = l$. The quantity $C(\alpha, l)$ defined in Lemma 1 is an upper bound on the number of non-zero polynomials $k \in \mathbb{F}_b[x]$ with $\deg_\alpha(k) = l$. Thus we have

$$A(l, s, \alpha) \leqslant \sum_{i=1}^{s} \binom{s}{i} \sum_{\substack{l_1,\ldots,l_i \geqslant 1 \\ l_1+\cdots+l_i=l}} \prod_{z=1}^{i} C(\alpha, l_z).$$

Now $\sum_{l=0}^{\varrho} A(l, s, \alpha)$ is a bound on the number of non-zero vectors $\boldsymbol{k} \in \mathbb{F}_b^s[x]$ with $\sum_{j=1}^s \deg_\alpha(k_j) \leqslant \varrho$. Hence the number of vectors $\boldsymbol{q} \in R_n^s$ for which $\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) < \varrho$ is bounded by $b^{ns-m} \sum_{l=0}^{\varrho} A(l, s, \alpha)$. Hence if this number is smaller than $b^{ns}$, that is if at least

$$b^{ns-m} \sum_{l=0}^{\varrho} A(l, s, \alpha) < b^{ns},$$

then there exists a vector $\boldsymbol{q} \in R_n^s$ with $\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \varrho$. Hence the result follows.

(2) We proceed as in (1), but we note that there are $|R_n| = b^n$ polynomials $q \in R_n$ to choose from and that for each non-zero vector $\boldsymbol{k} \in \mathbb{F}_b^s[x]$ there are at least $(s-1)b^{n-m}$ of these polynomials $q$ such that $\boldsymbol{k} \cdot \left(1, q, q^2, \ldots, q^{s-1}\right) \equiv a \pmod p$ for some $a$ with $\deg(a) < n - m$. If at least

$$(s-1)b^{n-m} \sum_{l=0}^{\varrho} A(l, s, \alpha) < b^n,$$

then there exists a $q \in R_n$ such that $\boldsymbol{q} \equiv \left(1, q, q^2, \ldots, q^{s-1}\right) \pmod p$ satisfies $\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \varrho$. Hence the result follows. □

Above we have shown the existence of polynomial lattices which are digital $(t, \alpha, \beta, n \times m, s)$-nets over $\mathbb{F}_b$ for which the quality parameter $t$ satisfies a certain condition. This follows from Theorem 2 together with Theorem 3. Note that in the search for a polynomial lattice we have to choose the value $\alpha$ up front. If we do not know the smoothness $\delta$ of the integrand, then it can happen that $\alpha \neq \delta$. Hence in order for the bound in Theorem 1 to apply we still need to know the figure of merit of some order $\alpha'$ of a polynomial lattice which was constructed using the parameter $\alpha$ (where possibly $\alpha \neq \alpha'$; the bound in Theorem 1 can then be used with $\lfloor \beta n \rfloor - t = \varrho_\delta$). Hence in the following we will establish a propagation rule for polynomial lattices.

**Theorem 4.** *Let $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ be a polynomial lattice with figure of merit $\varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q}))$. Then for all $\alpha' \geqslant \alpha$ we have*

$$\varrho_{\alpha'}(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q}))$$

*and for $1 \leqslant \alpha' \leqslant \alpha$ we have*

$$\varrho_{\alpha'}(\mathcal{S}_{p,m,n}(\boldsymbol{q})) \geqslant \frac{\alpha'}{\alpha} \varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q})) - 2.$$

**Proof.** First let $\alpha' \geqslant \alpha$. Then $\deg_{\alpha'}(k) \geqslant \deg_\alpha(k)$ for all $k \in \mathbb{F}_b[x]$ and hence the definition of the figure of merit implies the result. Let now $1 \leqslant \alpha' \leqslant \alpha$. Theorem 2 implies that the polynomial lattice $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ is a digital $(t, \alpha, \beta, n \times m, s)$-net over $\mathbb{F}_b$ with $t = \lfloor \beta n \rfloor - \varrho_\alpha(\mathcal{S}_{p,m,n}(\boldsymbol{q}))$. From a result

in [3] it follows that $\mathcal{S}_{p,m,n}(\boldsymbol{q})$ is also a digital $(t', \alpha', \beta', n \times m, s)$-net over $\mathbb{F}_b$ with $\beta' = \beta\alpha'/\alpha$ and $t' = \lceil t\alpha'/\alpha \rceil$. Using Theorem 2 again it follows that

$$\varrho_{\alpha'}(\mathcal{S}_{p,m,n}(\boldsymbol{q})) = \lfloor \beta' n \rfloor - t' = \lfloor \beta n \alpha'/\alpha \rfloor - \lceil t\alpha'/\alpha \rceil \geqslant \frac{\alpha'}{\alpha} \varrho_{\alpha}(\mathcal{S}_{p,m,n}(\boldsymbol{q})) - 2,$$

which is the desired result. □

## 4. Discussion

Combining Theorems 2 and 3 yields results on the existence of digital $(t, \alpha, \beta, n \times m, s)$-nets over $\mathbb{F}_b$ with, in certain cases, low $t$-value. Let us in the following, for fixed $b$ and integer $\alpha$, consider the case $n = \alpha m$ and $\beta = 1$, i.e., we study digital $(t, \alpha, 1, \alpha m \times m, s)$-nets over $\mathbb{F}_b$ or for short digital $(t, \alpha, \alpha m \times m, s)$-nets.

Theorem 3 (1) guarantees the existence of a digital $(t_1, \alpha, \alpha m \times m, s)$-net over $\mathbb{F}_b$, where

$$t_1 = \alpha m - \varrho_1 \tag{1}$$

and $\varrho_1$ is the maximal $\varrho$ such that $\Delta(s, \varrho, \alpha)$ as defined in Theorem 3 is less than $b^m$.

Furthermore, Theorem 3(2) guarantees the existence of a digital $(t_2, \alpha, \alpha m \times m, s)$-net $S_{p,m,\alpha m}(\boldsymbol{q})$ over $\mathbb{F}_b$ with $\boldsymbol{q} \equiv (1, q, q^2, \ldots, q^{s-1}) \pmod p$, where

$$t_2 = \alpha m - \varrho_2 \tag{2}$$

and $\varrho_2$ is the maximal $\varrho$ such that $\Delta(s, \varrho, \alpha) < b^m/(s-1)$.

We compare our existence results to explicit constructions of digital $(t, \alpha, \alpha m \times m, s)$-nets over $\mathbb{F}_b$. Given the generating matrices $C'_1, \ldots, C'_{s\alpha}$ of a digital $(t', m, s\alpha)$-net over $\mathbb{F}_b$, ([3], see also [2]) gives the construction principle of a digital $(t_3, \alpha, \alpha m \times m, s)$-net over $\mathbb{F}_b$ with

$$t_3 = \min\left\{ \alpha m, \alpha t' + s\frac{\alpha(\alpha-1)}{2} \right\}. \tag{3}$$

For several values of $\alpha, m, s$, and $b$, we computed the values of $t_1, t_2$, and $t_3$ given by (1), (2), and (3), respectively. Our numerical results are visualized in Figs. 1–4. The values of $t'$ for existing digital $(t', m, s\alpha)$-nets over $\mathbb{F}_b$ with explicitly computable generating matrices were taken from

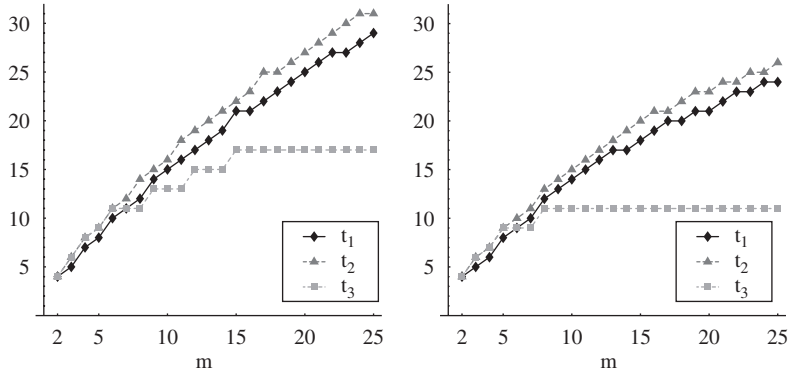


Fig. 1. $t$-values depending on $m$ $(2 \leqslant m \leqslant 25)$ for $s = 5$, $\alpha = 2$, and $b = 2$ (left), $b = 3$ (right).

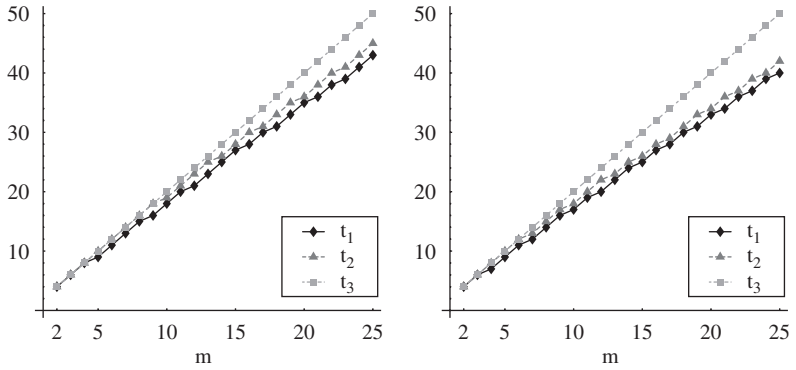


Fig. 2. $t$-values depending on $m$ ($2 \leqslant m \leqslant 25$) for $s = 25$, $\alpha = 2$, and $b = 2$ (left), $b = 3$ (right).

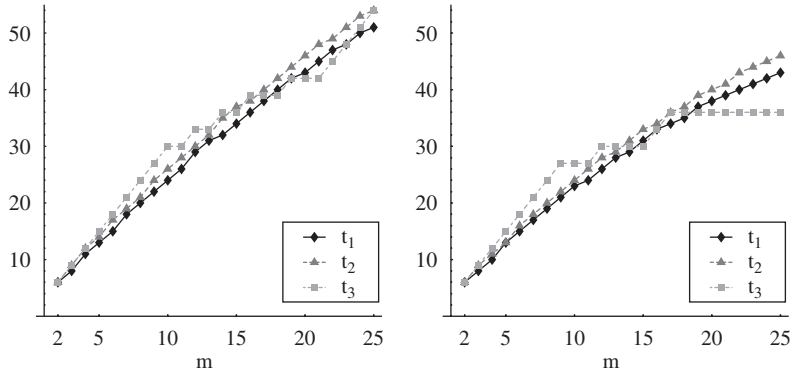


Fig. 3. $t$-values depending on $m$ ($2 \leqslant m \leqslant 25$) for $s = 5$, $\alpha = 3$, and $b = 2$ (left), $b = 3$ (right).

the web-based database system MINT (available at the address `http://mint.sbg.ac.at/`) for querying bounds on $(t, m, s)$-net and $(t, s)$-sequence parameters (see [13] for a recent outline).

From Figs. 1–4 we see that we frequently have $t_2 > t_1$, which occurs as the bound on $\Delta(s, \varrho_2, \alpha)$ is smaller than that on $\Delta(s, \varrho_1, \alpha)$ (point sets in Theorem 3 (2) ($\boldsymbol{q} \equiv (1, q, q^2, \ldots, q^{s-1}) \pmod p$)) are also special cases of those considered in Theorem 3 (1)). On the other hand, when performing a full search, generating vectors $\boldsymbol{q}$ of the form as in Theorem 3 (2) are more likely to be found than in the general case since the size of the search space is smaller. Overall, the difference between $t_1$ and $t_2$ can be said to be not very large.

The main conclusion to be drawn from Figs. 1–4 is that both $t_1$ and $t_2$ are lower than $t_3$ for higher dimensions and/or higher values of $\alpha$, whereas the opposite is the case for lower dimensions and/or lower values of $\alpha$. This is certainly caused by the term $s\alpha(\alpha - 1)/2$ in the formula for $t_3$ depending on $t'$. This "error term" becomes large as $s$ and $\alpha$ grow—it becomes so large that for higher dimension $t_3$ attains the maximal possible value $\alpha m$. Note that the term $s\alpha(\alpha-1)/2$ comes from an estimation which in general cannot be improved for the construction proposed in [2,3] unless one uses more information about the underlying digital $(t', m, s\alpha)$-net over $\mathbb{F}_b$ (it is possible on the other hand that the real $t$-value is actually smaller than the upper bound (3)). In [3] there

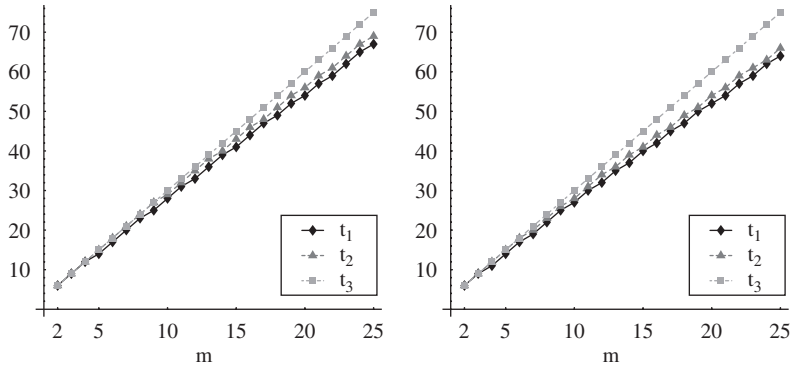


Fig. 4. $t$-values depending on $m$ ($2 \leqslant m \leqslant 25$) for $s = 25$, $\alpha = 3$, and $b = 2$ (left), $b = 3$ (right).

is also a lower bound (which again relates the $t$-value of a digital $(t, \alpha, \alpha m \times m, s)$-net over $\mathbb{F}_b$ to a digital $(t', m, s\alpha)$-net over $\mathbb{F}_b$), which is the same as the upper bound except for this additional term. From this it follows that the constructions in [2,3] leave some room for improvement and we have shown here that indeed there exist polynomial lattices which can in certain cases improve upon the construction in [2,3]. Unfortunately, our results here are not explicit as opposed to the results in [2,3].

## Acknowledgments

This work is supported by the Austrian Research Foundation (FWF), Project S 9609, that is part of the Austrian Research Network "Analytic Combinatorics and Probabilistic Number Theory", and Project P18455. The support of the ARC under its Center of Excellence program is gratefully acknowledged.

## References

[1] N. Aronszajn, Theory of reproducing kernels, Trans. Amer. Math. Soc. 68 (1950) 337–404.
[2] J. Dick, Explicit constructions of quasi-Monte Carlo rules for the numerical integration of high dimensional periodic functions, submitted for publication.
[3] J. Dick, Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order, submitted for publication.
[4] J. Dick, F. Pillichshammer, Strong tractability of multivariate integration of arbitrary high order using digitally shifted polynomial lattice rules, J. Complexity, 2007, to appear.
[5] G. Larcher, A. Lauss, H. Niederreiter, W.Ch. Schmid, Optimal polynomials for $(t, m, s)$-nets and numerical integration of multivariate Walsh series, SIAM J. Numer. Anal. 33 (1996) 2239–2253.
[6] P. L'Ecuyer, Polynomial integration lattices, in: H. Niederreiter (Ed.), Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer, Berlin, 2004, pp. 73–98.
[7] C. Lemieux, P. L'Ecuyer, Randomized polynomial lattice rules for multivariate integration and simulation, SIAM J. Sci. Comput. 24 (2003) 1768–1789.
[8] H. Niederreiter, Point sets and sequences with small discrepancy, Monatsh. Math. 104 (1987) 273–337.
[9] H. Niederreiter, Low-discrepancy point sets obtained by digital constructions over finite fields, Czechoslovak Math. J. 42 (1992) 143–166.
[10] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, CBMS-NSF Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, 1992.
[11] H. Niederreiter, Constructions of $(t, m, s)$-nets and $(t, s)$-sequences, Finite Fields Appl. 11 (2005) 578–600.

[12] W.Ch. Schmid, Improvements and extensions of the "Salzburg Tables" by using irreducible polynomials, in: H. Niederreiter, J. Spanier (Eds.), Monte Carlo and Quasi-Monte Carlo Methods 1998, Springer, Berlin, 2000, pp. 436–447.
[13] R. Schürer, W.Ch. Schmid, MinT: a database for optimal net parameters, in: H. Niederreiter, D. Talay (Eds.), Monte Carlo and Quasi-Monte Carlo Methods 2004, Springer, Berlin, 2006, pp. 457–469.
[14] I.H. Sloan, H. Woźniakowski, When are quasi-Monte Carlo algorithms efficient for high-dimensional integrals?, J. Complexity 14 (1998) 1–33.